

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

United States Patent and Trademark
Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year)

20 April 1999 (20.04.99)

International application No.

PCT/DE98/01943

Applicant's or agent's file reference

T97017 PCT

International filing date (day/month/year)

13 July 1998 (13.07.98)

Priority date (day/month/year)

04 August 1997 (04.08.97)

Applicant

DUPRE, Michael

1. The designated Office is hereby notified of its election made:



in the demand filed with the International Preliminary Examining Authority on:

26 February 1999 (26.02.99)



in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Diana Nissen

Telephone No.: (41-22) 338.83.38

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE 98/01943

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 6 H0407/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 H040

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 93 07697 A (COMVIK GSM AB) 15. April 1993 siehe Seite 3, Zeile 4 - Seite 7, Zeile 11 ---	1-9, 12
X	WO 97 14258 A (QUALCOMM INC) 17. April 1997 siehe Seite 10, Zeile 15 - Seite 21, Zeile 30 ---	1, 2, 5-10, 12
X	EP 0 481 714 A (VODAFONE LTD) 22. April 1992 siehe Spalte 3, Zeile 15 - Spalte 6, Zeile 9 ---	1-3, 11-13
X	EP 0 562 890 A (HUTCHISON MICROTEL LIMITED) 29. September 1993 siehe Spalte 2, Zeile 41 - Spalte 6, Zeile 57 ---	1

-/-

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

8. Dezember 1998

Absenddatum des internationalen Recherchenberichts

14/12/1998

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Bevollmächtigter Beauftragter

Robert 1. V

INTERNATIONALER RESEARCHBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Im Nationales Aktenzeichen

PCT/DE 98/01943

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9307697 A	15-04-1993	SE 468068 B	26-10-1992
		AU 661048 B	13-07-1995
		AU 2699092 A	03-05-1993
		CA 2115435 A,C	15-04-1993
		DE 606408 T	16-03-1995
		EP 0606408 A	20-07-1994
		FI 940804 A	21-02-1994
		JP 6511125 T	08-12-1994
		NO 940473 A	16-02-1994
		NZ 244523 A	27-02-1996
		SE 9102835 A	26-10-1992
		SG 44338 A	19-12-1997
		US 5557679 A	17-09-1996
WO 9714258 A	17-04-1997	AU 7442696 A	30-04-1997
		CA 2234558 A	17-04-1997
		EP 0855125 A	29-07-1998
EP 0481714 A	22-04-1992	GB 2248999 A	22-04-1992
		AT 147223 T	15-01-1997
		DE 69123931 D	13-02-1997
		DE 69123931 T	30-04-1997
		DK 481714 T	16-06-1997
		ES 2096635 T	16-03-1997
		FI 914917 A	18-04-1992
		GR 3022655 T	31-05-1997
		IE 65966 B	29-11-1995
		NO 180811 B	24-03-1997
		PT 99263 A	31-01-1994
EP 0562890 A	29-09-1993	KEINE	
EP 0820206 A	21-01-1998	BR 9703967 A	04-08-1998
		CA 2208601 A	15-01-1998
		JP 10117385 A	06-05-1998
		NO 973157 A	16-01-1998

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts T97017 PCT	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/DE 98/ 01943	Internationales Anmeldedatum (Tag/Monat/Jahr) 13/07/1998	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 04/08/1997
Anmelder DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. ☐ Bestimmte Ansprüche haben sich als nichtrecherchierbar erwiesen (siehe Feld I).
2. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).
3. ☐ In der internationalen Anmeldung ist ein Protokoll einer Nucleotid- und/oder Aminosäuresequenz offenbart; die internationale Recherche wurde auf der Grundlage des Sequenzprotokolls durchgeführt,
 - ☐ das zusammen mit der internationalen Anmeldung eingereicht wurde.
 - ☐ das vom Anmelder getrennt von der internationalen Anmeldung vorgelegt wurde,
 - ☐ dem jedoch keine Erklärung beigefügt war, daß der Inhalt des Protokolls nicht über den Offenbarungsgehalt der internationalen Anmeldung in der eingereichten Fassung hinausgeht.
 - ☐ das von der Internationalen Recherchenbehörde in die ordnungsgemäße Form übertragen wurde.
4. Hinsichtlich der Bezeichnung der Erfindung
 - ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
 - ☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt.
5. Hinsichtlich der Zusammenfassung
 - ☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.
 - ☐ wurde der Wortlaut nach Regel 38.2b) in der Feld III angegebenen Fassung von dieser Behörde festgesetzt. Der Anmelder kann der Internationalen Recherchenbehörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.
6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen:
Abb. Nr. _____
 - ☐ wie vom Anmelder vorgeschlagen
 - ☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.
 - ☐ weil diese Abbildung die Erfindung besser kennzeichnet.☒ keine der Abb.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 6 H04Q7/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 6 H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	WO 93 07697 A (COMVIK GSM AB) 15. April 1993 siehe Seite 3, Zeile 4 - Seite 7, Zeile 11 ---	1-9, 12
X	WO 97 14258 A (QUALCOMM INC) 17. April 1997 siehe Seite 10, Zeile 15 - Seite 21, Zeile 30 ---	1, 2, 5-10, 12
X	EP 0 481 714 A (VODAFONE LTD) 22. April 1992 siehe Spalte 3, Zeile 15 - Spalte 6, Zeile 9 ---	1-3, 11-13
X	EP 0 562 890 A (HUTCHISON MICROTREL LIMITED) 29. September 1993 siehe Spalte 2, Zeile 41 - Spalte 6, Zeile 57 ---	1
	--- -/--	



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfindnerischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindnerischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

8. Dezember 1998

Absendedatum des internationalen Recherchenberichts

14/12/1998

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Roberti, V

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	EP 0 820 206 A (AT & T WIRELESS SERVICES INC) 21. Januar 1998 siehe Spalte 4, Zeile 45 - Spalte 13, Zeile 42 -----	1,2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/DE 98/01943

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9307697	A	15-04-1993	SE 468068 B AU 661048 B AU 2699092 A CA 2115435 A,C DE 606408 T EP 0606408 A FI 940804 A JP 6511125 T NO 940473 A NZ 244523 A SE 9102835 A SG 44338 A US 5557679 A	26-10-1992 13-07-1995 03-05-1993 15-04-1993 16-03-1995 20-07-1994 21-02-1994 08-12-1994 16-02-1994 27-02-1996 26-10-1992 19-12-1997 17-09-1996
WO 9714258	A	17-04-1997	AU 7442696 A CA 2234558 A EP 0855125 A	30-04-1997 17-04-1997 29-07-1998
EP 0481714	A	22-04-1992	GB 2248999 A AT 147223 T DE 69123931 D DE 69123931 T DK 481714 T ES 2096635 T FI 914917 A GR 3022655 T IE 65966 B NO 180811 B PT 99263 A	22-04-1992 15-01-1997 13-02-1997 30-04-1997 16-06-1997 16-03-1997 18-04-1992 31-05-1997 29-11-1995 24-03-1997 31-01-1994
EP 0562890	A	29-09-1993	NONE	
EP 0820206	A	21-01-1998	BR 9703967 A CA 2208601 A JP 10117385 A NO 973157 A	04-08-1998 15-01-1998 06-05-1998 16-01-1998

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 12359.1-D1462-ne	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/DE98/01943	International filing date (day/month/year) 13 July 1998 (13.07.1998)	Priority date (day/month/year) 04 August 1997 (04.08.1997)
International Patent Classification (IPC) or national classification and IPC H04Q 7/38		
Applicant DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of <u>6</u> sheets, including this cover sheet. <input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT). These annexes consist of a total of <u>7</u> sheets.
3. This report contains indications relating to the following items: I <input checked="" type="checkbox"/> Basis of the report II <input type="checkbox"/> Priority III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability IV <input type="checkbox"/> Lack of unity of invention V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement VI <input type="checkbox"/> Certain documents cited VII <input type="checkbox"/> Certain defects in the international application VIII <input checked="" type="checkbox"/> Certain observations on the international application

Date of submission of the demand 26 February 1999 (26.02.1999)	Date of completion of this report 09 November 1999 (09.11.1999)
Name and mailing address of the IPEA/EP European Patent Office D-80298 Munich, Germany Facsimile No. 49-89-2399-4465	Authorized officer Telephone No. 49-89-2399-0

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/DE98/01943

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

- ☐ the international application as originally filed.
- ☒ the description, pages 1, 4-10, as originally filed,
pages _____, filed with the demand,
pages 2, 2a, 3, 11, filed with the letter of 21 October 1999 (21.10.1999),
pages _____, filed with the letter of _____.
- ☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-9, filed with the letter of 21 October 1999 (21.10.1999),
Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 1/2, 2/2, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims	1-9	YES
	Claims		NO
Inventive step (IS)	Claims	1-9	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-9	YES
	Claims		NO

2. Citations and explanations

1. The invention pertains to a **process** for personalizing GSM chips and a corresponding **chip** as per the features of the preamble to **Claims 1 and 6**, respectively.
2. In general GSM chips are either incorporated in a GSM card ("SIM"), which is plugged into a mobile telephone handset, or integrated permanently in the mobile telephone handset. Before the handset is commissioned, the network operator must personalize the GSM chip, wherein a card number (ICCID), a subscriber identifier (IMSI) and a plurality of secret keys are written in together with other data.

According to the hitherto generally applied **central** personalization process, the network operator receives blank cards from the card manufacturer, into which he writes the definitive secret key. This key is then stored only on the chip and in the network operator's authentication centre. Thus, at the moment of issue of the given card the authentication centre holds in store all subscriber identifiers and secret keys and has to administer these, although the given card is still with the

dealer and has not yet been sold. This type of GSM chip personalization is, on the one hand, unsafe and liable to abuse and, on the other, responsible for high administrative costs at the authentication centre.

EP-A-0 562 890 (D1) describes a similar process for personalizing GSM chips ("SIM") in mobile telephone handsets, wherein a remote update is carried out, enabling the control and access data stored on the GSM chip to be amended via the air interface. The IMSI, an ICCID and a secret key are stored on the GSM chip in the course of personalization.

In addition, **WO-A-97/14258** discloses a further process for programming a mobile telephone handset via the air interface, wherein programs in the mobile telephone handset may be updated or additional data transmitted to the mobile telephone handset. A secret key for ensuring transmission security is stored in both the mobile telephone handset and the authentication centre and serves to encode or decode transmitted data.

3. However, a significant **disadvantage** of the above indicated known processes is that they do not provide secure personalization of the GSM chip via the air interface.
4. The **technical problem** addressed by the present invention therefore consists in developing a process and a chip of the type described, for example, in D1 in such a way that secure personalization of the GSM chip via the air interface is possible and unnecessarily high administrative costs at the

authentication centre may be avoided.

5. A **process** for personalizing GSM chips and a corresponding **chip** as per the characterizing features of **Claims 1 and 6**, respectively, are provided to solve this **problem**.

The **invention** consists **essentially** in that the GSM chip is personalized on **initial check-in** by the subscriber to the subscriber network, wherein in a **first** step the chip derives an initial key from a key known to the chip manufacturer and input by him into the chip; in a **second** step an entry is made at the authentication centre and the home databank (HLR) as soon a subscriber has concluded a contract with the network operator; in a **third** step the authentication centre likewise derives the initial key; in a **fourth** step the network sets conditions whereby on checking-in to the network a connection is established between the chip and the security centre of the network operator; in a **fifth** step on first checking-in the connection between the chip and the security centre is activated; in a **sixth** step a new, second, secret key is negotiated with the chip or generated at the security centre and transmitted to the chip; and in a **seventh** step the conditions from the fourth step are deactivated again.

6. The invention has the **advantage** that, by effecting final personalization of the chip only after a contract has been concluded with the network operator, by avoiding preliminary entering at the authentication centre and by negotiating the (second) secret key on initial check-in to the

network, a more secure (final) personalization of the GSM chip via the air interface is possible and unnecessarily high administrative costs at the authentication centre are avoided.

7. The subject matter of the present invention is neither disclosed nor suggested by the other international search report citations, since in relation to the present invention these documents present only very general prior art in the technical field of GSM chips and the personalization thereof.
8. The subject matter of independent **Claims 1 and 6** is therefore considered to be **novel** and to involve an **inventive step** (PCT Article 33(2) and (3)).
9. **Claims 2-5 and 7-9** are dependent on Claims 1 and 6, respectively, and therefore **likewise** meet the requirements of PCT Article 33(2) and (3) with respect to **novelty** and **inventive step**.
10. The present invention is obviously also **industrially applicable** (PCT Article 33(4)).

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

1. Line 17 of **Claim 1** should read: "... initial, first key Ki_1 ..." (PCT Article 6).
2. **Claim 5** should refer back only to **Claim 4** since "... the hotlining flag..." in **Claim 5** is first disclosed in **Claim 4** (PCT Article 6).
3. **Claim 9** should refer back only to **Claims 6-8**, since only these claims pertain to the chip (PCT Article 6).

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM
GEBIET DES PATENTWESENS

PCT

REC'D 11 NOV 1999

WIPO PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts 12359.1-D1462-ne	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/DE98/01943	Internationales Anmeldedatum (Tag/Monat/Jahr) 13/07/1998	Prioritätsdatum (Tag/Monat/Tag) 04/08/1997
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04Q7/38		
Anmelder DETEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH et al.		



1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt sieben Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☐ Bestimmte Mängel der internationalen Anmeldung
- VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 26/02/1999	Datum der Fertigstellung dieses Berichts 09.11.1999
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Rabe, M Tel. Nr. +49 89 2399 8801 

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/DE98/01943

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1,4-10 ursprüngliche Fassung

2,2a,3,11 eingegangen am 23/10/1999 mit Schreiben vom 21/10/1999

Patentansprüche, Nr.:

1-9 eingegangen am 23/10/1999 mit Schreiben vom 21/10/1999

Zeichnungen, Blätter:

1/2,2/2 ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

3. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-9
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1-9
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-9
	Nein: Ansprüche	

2. Unterlagen und Erklärungen

siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

A. Bemerkungen zu Abschnitt V:

1. Die Erfindung bezieht sich auf ein **Verfahren** zur Personalisierung von GSM-Chips, sowie auf einen entsprechenden **Chip** gemäß den Merkmalen des Oberbegriffs von **Anspruch 1 bzw. 6**.
2. **Generell** sind GSM-Chips entweder in einer GSM-Karte (sog. SIM) implementiert, die in ein Mobilendgerät eingesteckt wird, oder fest in das Mobilendgerät integriert. Vor der Inbetriebnahme des Mobilendgerätes ist eine Personalisierung des GSM-Chips durch den Netzbetreiber erforderlich, wobei in den GSM-Chip neben anderen Daten eine Kartennummer (ICCID), eine Teilnehmerkennung (IMSI) und mehrere geheime Schlüssel eingeschrieben werden.

Bei der bisher allgemein angewandten **zentralen** Personalisierung bekommt der Netzbetreiber Rohkarten vom Kartenhersteller und schreibt dann den endgültigen geheimen Schlüssel hinein. Dieser Schlüssel ist dann nur auf dem Chip und im Authentifikationszentrum des Netzbetreibers abgespeichert. Das Authentifikationszentrum hat somit im Moment der Herausgabe der jeweiligen Karte alle Teilnehmerkennungen und geheimen Schlüssel gespeichert und muß diese verwalten, obwohl die jeweilige Karte noch beim Händler liegt und noch gar nicht verkauft worden ist. Diese Art der Personalisierung von GSM-Chips ist einerseits unsicher und mit der Gefahr des Mißbrauchs behaftet, und beansprucht andererseits einen großen Verwaltungsaufwand im Authentifikationszentrum.

Die **EP-A-0 562 890** beschreibt ein ähnliches Verfahren zur Personalisierung von GSM-Chips (sog. SIM) in Mobilendgeräten, wobei ein Fern-Update durchgeführt wird, über das eine Änderung der auf dem GSM-Chip gespeicherten Steuerungs- und Zugriffsdaten über die Luftschnittstelle ermöglicht. Auf dem GSM-Chip sind die IMSI, eine ICCID sowie ein geheimer Schlüssel im Zuge der Personalisierung gespeichert.

Darüber hinaus offenbart die **WO 97/14258** ein weiteres Verfahren zur Programmierung eines Mobilendgerätes über die Luftschnittstelle, wobei Programme in dem Mobilendgerät erneuert oder zusätzliche Daten an das Mobilendgerät übertragen werden können. Ein geheimer Schlüssel zur Gewährleistung der Übertra-

gungssicherheit ist sowohl im Mobilendgerät als auch im Authentifikationszentrum gespeichert und dient der Verschlüsselung bzw. Entschlüsselung der übertragenen Daten.

3. Ein wesentlicher **Nachteil** der oben angegebenen bekannten Verfahren besteht jedoch darin, daß keine sichere Personalisierung des GSM-Chips über die Luftschnittstelle vorgesehen ist.
4. Der vorliegenden Erfindung liegt somit die **Aufgabe** zugrunde, ein Verfahren bzw. einen Chip der z.B. in der EP-A-0 562 890 beschriebenen Art so weiterzubilden, daß eine sichere Personalisierung des GSM-Chips über die Luftschnittstelle möglich ist und daß ein unnötig großer Verwaltungsaufwand im Authentifikationszentrum vermieden werden kann.
5. Zur **Lösung** dieser Aufgabe ist ein **Verfahren** zur Personalisierung von GSM-Chips, sowie ein entsprechender **Chip** gemäß den kennzeichnenden Merkmalen **Anspruch 1 bzw. 6** vorgesehen.

Die **Erfindung** besteht **im wesentlichen** darin, daß die Personalisierung des GSM-Chips **beim erstmaligen** Einbuchen des Teilnehmers in das Teilnehmernetz erfolgt, wobei in einem **ersten** Schritt der Chip sich aus einem Schlüssel, den der Chiphersteller kennt und in den Chip einbringt, einen initialen Schlüssel ableitet, in einem **zweiten** Schritt ein Eintrag in das Authentifikationszentrum und die Heimatdatenbank (HLR) erfolgt, sobald ein Teilnehmer einen Vertrag mit dem Netzbetreiber geschlossen hat, in einem **dritten** Schritt sich das Authentifikationszentrum ebenfalls den initialen Schlüssel ableitet, in einem **vierten** Schritt das Netz Bedingungen setzt, damit beim Einbuchen ins Netz eine Verbindung vom Chip zum Security Center des Netzbetreibers entsteht, in einem **fünften** Schritt beim ersten Einbuchen die Verbindung vom Chip zum Security Center geschaltet wird, in einem **sechsten** Schritt im Security Center ein neuer, zweiter, geheimer Schlüssel mit dem Chip ausgehandelt oder erzeugt wird und zum Chip übertragen wird, und in einem **siebten** Schritt die Bedingungen aus dem vierten Schritt wieder ausgeschaltet werden.

6. Die Erfindung bietet den **Vorteil**, daß durch die Endpersonalisierung des Chips

erst nach Vertragsabschluß mit dem Netzbetreiber, durch das Vermeiden von Vorabenträgen im Authentifikationszentrum, sowie durch das Aushandeln des (zweiten) geheimen Schlüssels beim erstmaligen Einbuchen ins Netz, eine sichere (End-)Personalisierung des GSM-Chips über die Luftschnittstelle möglich ist und ein unnötig großer Verwaltungsaufwand im Authentifikationszentrum vermieden wird.

7. Der Gegenstand der vorliegenden Erfindung wird auch durch die weiteren, im Internationalen Recherchenbericht genannten Dokumente weder offenbart, noch nahegelegt, da diese Dokumente lediglich einen in bezug auf die vorliegende Erfindung sehr allgemeinen Stand der Technik im Fachgebiet der GSM-Chips und entsprechender Personalisierung darstellen.
8. Der Gegenstand der unabhängigen **Ansprüche 1 und 6** wird daher als **neu** und **erfinderisch** angesehen, Artikel 33 (2) und (3) PCT.
9. Die **Ansprüche 2 bis 5 bzw. 7 bis 9** sind abhängig von Anspruch 1 bzw. 6 und erfüllen somit **ebenfalls** die Erfordernisse des Artikels 33 (2) und (3) PCT hinsichtlich **Neuheit** und **erfinderischer Tätigkeit**.
10. Die vorliegende Erfindung ist offensichtlich auch **gewerblich anwendbar**, Artikel 33 (4) PCT.

B. Bemerkungen zu Abschnitt VIII:

1. Zeile 17 von **Anspruch 1** hätte lauten sollen: "... initialen, **ersten Schlüssel** Ki_1 ..." (Artikel 6 PCT).
2. **Anspruch 5** hätte sich lediglich auf Anspruch 4 beziehen sollen, da "... **das** Hot-lining flag ..." in Anspruch 5 erstmals in Anspruch 4 offenbart ist (Artikel 6 PCT).
3. **Anspruch 9** hätte sich lediglich auf die Ansprüche 6 bis 8 beziehen sollen, da nur diese Ansprüche den Chip betreffen (Artikel 6 PCT).

Schlüssel ist dann nur zwei Stellen bekannt, nämlich dem Chip selbst und dem Netzbetreiber.

Nachteilig hierbei ist, daß im Rechenzentrum des Netzbetreibers eine außerordentlich hohe statische Last erzeugt wird. Mit einem Generator werden eine Vielzahl von Schlüsseln erzeugt, die dann in die jeweiligen Karten eingebracht werden. Man schickt dann gleichzeitig den jeweils pro Karte erzeugten Schlüssel zum Rechenzentrum (Authentifikationszentrum AC), und danach wird den Karte an die Verkaufsorganisationen herausgegeben. Das AC hat also im Moment der Herausgabe der jeweiligen Karte bereits alle Teilnehmerkennungen IMSI und die dazugehörenden geheimen Schlüssel Ki gespeichert und muß diese verwalten, obwohl die jeweilige Karte noch irgendwo beim Händler liegt und noch gar nicht verkauft worden ist. Bei einer größeren Anzahl von Verkaufsstellen liegen also Karten, die noch nicht verkauft wurden und deren Daten aber trotzdem vom AC verwaltet werden müssen.

Außerdem besteht prinzipiell die Gefahr, daß wenn ein Hersteller oder irgendein anderes Mitglied der Verkaufsorganisation die Karten personalisieren soll, es sein könnte, daß dieser Schlüssel kompromittiert ist. Die anfängliche Personalisierung des Chip ist also unsicher und mit der Gefahr des Mißbrauchs behaftet.

Die EP-A-562 890 offenbart ein mobiles Kommunikationsnetz mit der Möglichkeit eines Fern-Update eines sogenannten Teilnehmer-Identitätsmodules (SIM) in Mobilstationen. Die SIM speichert Daten für die Steuerung der Mobilstationen und den Zugriff auf die Dienste des Mobilfunknetzes. Die auf der SIM gespeicherten Daten können nun auf der Funkschnittstelle geändert, d.h. upgedated werden. Ein Verfahren zur Personalisierung einer SIM über die Luftschnittstelle ist hier jedoch nicht beschrieben.

Aus der WO-A-97/14258 ist ebenfalls ein Verfahren und eine Vorrichtung für die Programmierung einer Mobilstation über die Luftschnittstelle bekannt. Hierbei werden bei Bedarf eingespeicherte Programme in der Mobilstation erneuert bzw. zusätzliche Daten über die Luftschnittstelle übertragen. Mit den hier beschriebenen Verfahren ist außerdem eine erstmalige Aktivierung der Mobilstation über die Luftschnittstelle möglich, nicht jedoch die Personalisierung eines Teilnehmeridentitätsmoduls.

Die WO-A-93/07697 betrifft ein Verfahren für die Personalisierung einer aktiven sogenannten SIM-Karte. Hierbei findet die komplette Personalisierung der SIM-Karte in einem autorisierten Terminal statt, welches über eine verschlüsselte Kommunikationsleitung mit dem zentralen Computer des Mobilfunknetzwerkes verbunden ist. Eine Personalisierung der Chipkarte beim erstmaligen Einbuchen des Teilnehmers in das Mobilfunknetz ist auch aus dieser Schrift nicht zu entnehmen.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren, eine Vorrichtung und einen Chip der eingangs genannten Art so weiterzubilden, daß ein unnötig großer Verwaltungsaufwand im AC entfallen kann und daß die Aufbewahrung der geheimen Daten des Chip sicherer ausgebildet ist.

Zur Lösung der gestellten Aufgabe ist die Erfindung durch die technische Lehre des Anspruchs 1 gekennzeichnet. Ein Chip nach der Erfindung ist durch die technische Lehre des Anspruchs 6 gekennzeichnet.

Mit der erfindungsgemäßen technischen Lehre werden insbesondere folgende Vorteile erreicht :

- Vermeidung einer zentralen Personalisierung beim Netzbetreiber
- Ausgabe von sehr vielen GSM-Chips ohne Erzeugung einer statischen Last beim Netzbetreiber
- Wiederverwendung von "gebrauchten" GSM-Chips
- Regelmäßiger Wechsel des secret Key Ki während der Nutzungsdauer durch den Kunden.

Mit dem hier vorgestellten Verfahren bringt der Gerätehersteller/Chiphersteller initiale kartenbezogene Daten in den Chip ein, sozusagen eine Vorpersonalisierung. Die eigentliche Personalisierung nimmt der Netzbetreiber selbst zu einem späteren Zeitpunkt vor, und auch nur bei den Kunden, die ein Vertragsverhältnis mit dem Netzbetreiber eingehen.

Die Vorpersonalisierung erzeugt bei dem Netzbetreiber noch keine statische Last. Das Verfahren bietet somit die Voraussetzung, um "Millionen" von GSM-Chips zu verteilen, z. B. in jedes Auto, in jeden Laptop oder in jede Alarmanlage, und später nur die Chips der Kunden zu "aktivieren", die ein Vertragsverhältnisse eingehen.

Des weiteren ist es möglich, Karten wiederzuverwenden, falls ein Kunde sein Vertragsverhältnis kündigt (z. B. bei Verkauf seines Autos).

Speziell beim Netzbetreiber D1 könnte der Händler zurückgegebene Karten erneut für einen anderen Kunden freischalten. Der Netzbetreiber spart somit die Personalisierung von Karten für das Austauschgeschäft ein.

AMENDED SHEET

Das SC teilt im vierten Verfahrensschritt gleichzeitig die geheime Schlüsselzahl Ki_2 dem AC mit.

Damit ist die Karte freigeschaltet und endpersonalisiert.

Die Wiederverwendung gebrauchter Karten ist weiter oben näher dargestellt. Hierbei ist in Figur 3 erkennbar, daß der Kunde mit seiner Karte sich an die VO wendet, welche durch Eintragung der Kartennummer ICCID in die Auftragsbestätigung dafür sorgt, daß im AC die IMSI gelöscht wird und gleichzeitig auch im HLR.

Damit wird auch die Ki_2 gelöscht und die Ki_1 wird wieder aktiviert und in die Karte eingespeichert. Ebenso wird die PIN auf den Wert 0000 gesetzt und ebenfalls die PUK.

Die so wieder vorpersonalisierte Karte kann denn in einen Kartenpool eingestellt werden und für neue Kunden vergeben werden.

Die Endpersonalisierung wurde also wieder rückgängig gemacht und es liegt wieder der Zustand der Karte vor, wie er zum Zeitpunkt der Vorpersonalisierung bestand.

Es sei noch angemerkt, daß die Stelle des Netzbetreibers, bei welcher die Auftragsbestätigung abgewickelt wird, als Auftragsannahmestelle bezeichnet wird und diese Auftragsannahmestelle kennt die Zuordnungen von ICCID zu IMSI wegen der 1:1-Zuordnung innerhalb des vergebenen Nummernbereiches.

AMENDED SHEET

1. Verfahren zur Personalisierung von GSM-Chips, in deren Speicherbereich mindestens eine Teilnehmer-Kennung IMSI, eine
5 Kartenummer ICCID und zwecks Personalisierung ein geheimer Schlüssel Ki und gegebenenfalls weitere Daten eingespeichert werden, wobei zur Vorpersonalisierung des Chips beim Hersteller zunächst initiale, kartenbezogene Daten, nämlich ein erster, geheimer Schlüssel Ki_1 und gegebenenfalls
10 weitere Daten, wie PIN und PUK eingespeichert werden, **dadurch gekennzeichnet**, daß die Personalisierung des Chips dann erfolgt, wenn der Teilnehmer sich erstmals in das Teilnehmernetz einbucht, wobei folgende Verfahrensschritte durchlaufen werden:
- 15 - in einem ersten Verfahrensschritt entnimmt der Chiphersteller die ICCID und IMSI einem Nummernpool, der Chip selbst leitet sich aus einem Schlüssel K1, den der Chiphersteller kennt und in den Chip einbringt, einen initialen Ki_1 ab, PIN und PUK werden auf einen Defaultwert
20 gesetzt;
 - in einem zweiten Verfahrensschritt erfolgt ein Eintrag im Authentifikationszentrum (AC) und der Heimatdatenbank (HLR), sobald ein Teilnehmer einen Vertrag mit dem Netzbetreiber geschlossen hat;
 - 25 - in einem dritten Verfahrensschritt leitet sich das Authentifikationszentrum (AC) ebenfalls den initialen, ersten Schlüssel Ki_1 ab;
 - in einem vierten Verfahrensschritt setzt das Netz die Bedingungen, damit beim Einbuchen ins Netz eine Verbindung
30 vom Chip zum Security Center des Netzbetreibers (SC) entsteht;
 - in einem fünften Verfahrensschritt wird beim ersten Einbuchen die Verbindung vom Chip zum Security Center (SC) geschaltet;
 - 35 - in einem sechsten Verfahrensschritt wird im Security Center (SC) ein neuer, zweiter, geheimer Schlüssel Ki_2, sowie gegebenenfalls ein PUK mit dem Chip ausgehandelt oder im Security Center (SC) erzeugt und zum Chip übertragen;
 - in einem siebten Verfahrensschritt werden die Bedingungen
40 aus dem vierten Verfahrensschritt wieder ausgeschaltet.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der
erstmalig in den Chip eingespeicherte, initiale, geheime
Schlüssel Ki_1 vor Vertragsabschluß nicht in das
5 Authentifikationszentrum (AC) übertragen und dort gespeichert
wird.
3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß zum
Aushandeln des zweiten, geheimen Schlüssels Ki_2 ein
10 Verfahren nach Diffie-Hellman verwendet wird.
4. Verfahren nach einem der Ansprüche 1-3, dadurch
gekennzeichnet, daß die Heimatdatenbank (HLR) geeignet ist,
einen Umleitungsbefehl (Hotlining-Flag) zu setzen und zu
15 löschen.
5. Verfahren nach einem der Ansprüche 1-4, dadurch
gekennzeichnet, daß mit der erstmaligen Eintragung des
initialen Schlüssel Ki_1 in das Authentifikationszentrum (AC)
20 auch das Hotlining flag in der Heimatdatenbank (HLR) gesetzt
wird.
6. Chip zur Ausübung des Verfahrens nach einem der Ansprüche
25 1 bis 5, in dessen Speicherbereich mindestens eine
Teilnehmer-Kennung IMSI und eine Kartenummer ICCID und
zwecks Personalisierung ein geheimer Schlüssel Ki und
gegebenenfalls weitere Daten eingespeichert sind, wobei zur
Vorphonalisierung des Chips ferner initiale, kartenbezogene
30 Daten, nämlich ein erster, geheimer Schlüssel Ki_1 und
gegebenenfalls weitere Daten, wie PIN und PUK eingespeichert
sind, **dadurch gekennzeichnet,**
daß der Chip im Endgerät toolkitfähig ist, und Mittel
aufweist, mit welchen er mit einem Security Center (SC)
35 kommunizieren und einen Schlüssel aushandeln kann.
7. Chip nach Anspruch 6, dadurch gekennzeichnet, daß er
Mittel aufweist, mit denen er Daten aus dem Security Center
(SC) empfängt und diese in einen Speicher einschreibt und

gegebenenfalls aus dem Speicher ausliest, verändert und/oder an das Security Center (SC) überträgt.

- 5 8. Chip nach einem der Ansprüche 6 oder 7, dadurch gekennzeichnet, daß er einen Mikroprozessor zum Aushandeln eines geheimen Schlüssels mit dem Security Center (SC) aufweist.
- 10 9. Chip nach einem der Ansprüche 5-8, dadurch gekennzeichnet, daß er eine vom Hersteller fest programmierte Rufnummer enthält (fixed dialing).

09 / 4 8 5 3 5 2

420 Rec'd PCT/PTO 0 4 FEB 2000

To the Assistant Commissioner of Patents

I, the below-named translator, hereby declare that:

My name and post office address are as stated below;

That I am knowledgeable in the English language and in the language in which the below-identified PCT application was filed, and that I believe the English translation of the PCT application Method and device for customer personalization of GSM chips is a true and complete translation of the above identified PCT application as filed (PCT/DE98/01943; Atty. Docket No. 2643/0G629).

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Date: January 26, 2000

Wolfgang E. Stutius

Name of the translator



Signature of the translator

80 Country Drive
Weston, MA 02493-1165

Post Office Address

Method and device for customer personalization of GSM chips

Description

- 5 A method is proposed for customer personalization of GSM chips which assumes that the chip at the time of the personalization is located in the terminal equipment of the customer.

According to the present state of the art, the network operators presently implement the GSM chip in a GSM card which is inserted in the terminal equipment. The chip may
10 also be permanently integrated in the terminal equipment, for example, on a plug-in card of a computer. It is not important for the present method if a GSM card or a terminal with an integrated chip is employed. A "chip" in the broadest sense is understood to be an EPROM, an EEPROM, as well as an "intelligent" microprocessor.

- 15 Regardless of a particular embodiment, the following discussion will use the term "chip" and "chip manufacturer."

With centralized personalization used until now, the chip receives, aside from other data, a card number (ICCID), a subscriber identification number (IMSI) as well as
20 several secret numbers. While the chip manufacturer can easily apply the data ICCID and IMSI to the chip, the network operator likes to keep control over the secret numbers, in particular over the key Ki, which should be known only to the card and the network.

- 25 With the present centralized personalization, the network operator receives from the card manufacturer unmarked cards and subsequently writes the final secret key.

EXPRESS MAIL CERTIFICATE

2/4/2000
Date Label No. 503340143

I hereby certify that, on the date indicated above I deposited this paper or fee with the U.S. Postal Service & that it was addressed for delivery to the Commissioner of Patents & Trademarks, Washington D.C. 20591 by "Express Mail Post Office to Addressee" service.

D Beck
Name (Print)

Signature

Accordingly, this key is only known to two localities, namely the chip itself and the network operator.

Disadvantageously, an extraordinarily large static load is produced in the computer center of the network operator. A generator generates a large number of keys which
5 are then applied to the respective cards. The key generated for each card is then simultaneously transmitted to the computer center (authentication center AC), whereafter the card is issued to the sales organization. The AC therefore has already stored all subscriber identification numbers IMSI and the associated secret keys Ki at the time the respective card is issued and has to administer these identification
10 numbers and keys, although the respective card has not yet been sold and is still in the possession of the vendor. Consequently, cards which have not yet been sold are stored in large numbers of sales offices, while the data of these cards have to be administered by the AC.

15 In addition, it may happen that when a manufacturer or another member of the sales organization attempts to personalize the cards, the key may have already be compromised. The initial personalization of the chip is therefore not secure and may be subject to misuse.

20 It is therefore an object of the invention to improve a method, a device and a chip of the aforescribed type so that the overly complex administration in the AC can be simplified and the secret data of the chip can be stored more securely.

To solve the object, the invention is characterized by the technical teachings of claim
25 1. A chip according to the invention is characterized by the technical teachings of the claims 6 to 10. Furthermore, the device for customer personalization of the GSM chip is described in the claims 11 to 13.

The technical teachings according to the invention attains the following advantages:

Elimination of a central personalization at the network operator

Issuance of a large number of GSM chips without producing a static load at the

5 network operator

Reuse of "used" GSM chips

Regular change of the secret key Ki while in use by the customer.

10 With the proposed method, the device manufacturer/chip manufacturer applies initial data associated with the card to the chip, which could be referred to as pre-personalization. The network operator himself performs the actual personalization at a later time and only for those customers who enter into a contract with the network operator.

15 The pre-personalization does not yet produce a static load at the network operator. The method therefore makes it possible to distribute "millions" of GSM chips, for example in each and every automobile, in each laptop computer or in each alarm system, and to subsequently "activate" only the chips of those customers who enter into a contract.

20 It is also possible to reuse cards if a customer terminates his contract (for example, if he sells his automobile).

In particular, in the case of the network operator D1, the dealer could release returned cards again for another customer. The network operator therefore eliminates the
25 personalization of cards in the terminal equipment replacement business.

To implement the technical teachings, the GSM chip can advantageously be Toolkit-enabled. In particular, the terminal equipment should be able to transmit short messages to the network operator. The chip should also offer a function to restore the initial state of the chip (see below).

- 5 The terminal equipment or a different device may also use this function of the chip. The terminal equipment should also be able to read the card number and the version number (see below). (Alternatively, the card number and the version number could be indicated on the GSM card).

- 10 The chip manufacturer is responsible for the pre-personalization. ICCID and IMSI are taken from a pool of numbers, whereas the chip itself derives from a key K_1 which is known to the chip manufacturer, an initial key K_{i_1} . PIN and PUK are set to a default value.

No entry is made into the AC

- 15 When a customer is signed up, an entry is made in the AC. This entry is also derived from the initial key K_{i_1} .

The hotlining flag is set in the HLR

The first call is routed to a security center

- The security center negotiates a new K_{i_2} as well as a PUK, using the Diffie-Hellman
20 method.

Used chips intended for reuse are reset with an internal function.

- Pre-personalization at the chip manufacturer is carried out by allocating a range of card numbers and subscriber identification numbers to each chip manufacturer. The
25 number ranges for ICCID and IMSI are large enough to make this possible.

The chip manufacturer also receives the following data from the network operator: a, p, VER, K_1 .

The chip manufacturer then applies the following data to each chip:

ICCID card number

IMSI subscriber identification number (is tied to ICCID, for example, by having the same position within the two number ranges for ICCID and IMSI)

a a sufficiently large number forming the basis for Diffie-Hellman

5 p a sufficiently large number, prime number for Diffie-Hellman

VER a version number, for example 8 bytes, unique for each chip manufacturer (can be changed from time to time)

K1 8 bytes DES key, uniquely tied to VER.

10 Note: The network operator could derive the key K1 from the version number VER using a master key (for example with the DES method).
However, this is not required.

The chip then generates the following secret numbers:

15

Ki_1 Ki_1 is an initial Ki which the chip derives from the IMSI using the DES key K1.

PIN PIN is set to a fixed value of 0000.

PUK PUK is set to a fixed value of 00000000.

20 Optionally, additional secret numbers.

The chip must retain K1 and the generated secret numbers in a secure region and protect these numbers from being read.

25 The processes in the authentication center AC:

The AC knows the key K1 of each version number VER (K1 can be derived from VER using a master key so that the values K1 issued to the chip manufacturer do not need to be stored).

30 The initial values Ki_1 generated by the chips are not recorded in the AC.

Since the AC does not yet know the IMSI's, no static load is produced.

Customer sign-up and release by the network operator

- 5 A customer who wishes to use his device (his card, his chip), enters into a contract with the network operator. The card number (ICCID) identifies the chip.

The network operator activates the following actions:

- 10 Reading or obtaining the card number and version number (ICCID, VER)
 The IMSI is permanently associated with the ICCID
 IMSI and VER are entered into the AC (it is only now that the subscriber relationship is made known in the AC)
 The AC knows the key K1 which is permanently tied to VER and generates from K1
 15 the initial key Ki_1 from the IMSI, using the same method being used in the chip
- The HLR sets the "hotlining flag" to this IMSI. The first call is then routed to an SC (security center). (The SC could also be the HLR/AC itself)
- 20 The first call: final personalization of the chip

Since the chip and the AC now have knowledge of the same secret key Ki_1, the chip logs on to the network. (The PIN is 0000 and known to the customer)

- With hotlining enabled, the first call is automatically routed to the SC. Depending on
 25 the software in the Toolkit-enabled terminal equipment, the first call could already be a short message

The SC advantageously uses the Toolkit-features of the chip and negotiates with the chip a new secret key Ki_2.

The Diffie-Hellman method is used herein which has the following advantages:

Keys of arbitrary length can be negotiated

It is not sufficient to listen to the air interface to extract the generated key.

The chip stores the new key Ki_2 (this key is subsequently used for authentication).

- 5 - The new key can be immediately verified (for example, challenge response, as is customary with GSM);
- The SC transmits the new key Ki_2 to the AC;
- By again using Diffie-Hellman, the SC negotiates a PUK (or additional secret numbers) with the chip. (The network operator can subsequently communicate the
- 10 secret numbers to the customer or retain the secret numbers for service purposes)
- The hotlining flag in the HLR is removed. Normal calls are now enabled, with the new secret key Ki_2 being used from this time on;
- The Toolkit-enabled terminal equipment informs the customer about success or failure;
- 15 - The Toolkit-enabled terminal equipment may ask the customer to select a new PIN.

Reuse of used chips/cards

- 20 It will be assumed that the subscriber relationship is removed from the HLR and the AC because the customer has terminated his contract. When a contract is entered with the new customer and a used chip is reused, the following steps are executed:

First, the function of the terminal equipment to initialize the chip is employed.

Thereafter, in the chip:

- 25 Ki_2 is deleted
- Ki_1 is reactivated
- The PIN is set to 0000
- The PUK is set to 00000000 (in an analogous manner, with additional secret numbers PUK2)
- 30 This function could, for example, be activated within the D1 network by the X13 which is installed at many dealer sites. In this way, the dealer can issue another initialized card.

The additional steps are identical to those for customer sign-up and release by the

network operator (see above).

Change of the secret key during the utilization time of the chip

- 5 The network operator can force a change of Ki in regular intervals. This can be done simply by enabling the hotlining flag in the HLR which routes the call to the SC and, as described above, by negotiating a new Ki. However, the PUK should not be renegotiated at this time.

10 Possibilities for misuse (illustrated here for D1)

1. The key K1 of a chip manufacturer is compromised and a card is copied.

- 1.1 The IMSI is not yet known in the AC. The card does not register.

- 15 1.2 The IMSI of the genuine card is already in the AC and has already been provided with the final personalization.

The forged card cannot log on since Ki_1 is different from Ki_2 (authentication failed).

- 20 1.3 The genuine IMSI is already in the AC, but final personalization has not yet been performed.

This refers to the brief time interval between the time the contract takes effect and the device is switched on for the first time. During this time interval, a forged card could be "inserted." The genuine card would then not be able to log on because it does not have the Ki_2 of the forged card. This scenario could be prevented, for example,

25

by including - at the time of the subscription - on the order document a secret number which the customer has to provide after receiving the key. This secret number is sent to the SC where it is checked.

- 5 2. The customer initializes his own card (for example with X13). Thereafter, the card has the key Ki_1 and does no longer log on.

The invention will now be described with reference to an embodiment illustrated in the drawings. Additional features and advantages are disclosed in the drawings and in the
10 description of the drawings.

It is shown in:

Figure 1: schematically, the pre-personalization of the cards at the chip manufacturer;
15

Figure 2: schematically, the processes during the release by the network operator (final personalization);

Figure 3: schematically, the processes when the chip is erased and reused.
20

Figure 1 illustrates in the form of a drawing what has already been described on page 4 of the description, namely that the card number ICCID is provided in a range between a number X and a number Y.

25 The same applies to the subscriber identification number IMSI which is also located in a range of values between A and B.

In the two number ranges allocated for ICCID and IMSI, a number a is selected as a base for the Diffie-Hellman algorithm as well as a number p which serves as a prime
30 number for the Diffie-Hellman encryption.

Also defined is a number VER which can be a functional number having a length of 8 bytes. In addition, the key X1 is computed in form of a DES key which is tied to VER.

- 5 The aforescribed data are entered into the card, with the chip generating (computing) the secret number Ki_1 which is stored in the card. The card is supplied in this form (pre-personalized) to the VO (sales organization).

10 Figure 2 illustrates the individual processes which are described in the description starting on page 5 .

In a first process step, the VO enters into a contract with the customer. In the same process step, the card number ICCID and the version number together with the contract are entered in an order confirmation, wherein this order confirmation is
15 communicated in a second process step to the AC together with the subscriber identification number and the version number VER.

At the same time, the subscriber identification number IMSI is communicated to the HLR so that the HLR is made aware of the card data and establishes the so-called
20 hotlining flag.

The customer now receives his pre-personalized card and establishes in a first call - which according to the present invention is forcibly switched to the SC - contact with the SC. In this first call, the Ki_2 is negotiated as well as the PUK, with the new PIN
25 being set at the same time. At the same time, the SC verifies the secret key Ki_2 with respect to the card.

In a fourth method step, the SC contacts the HLR and removes the hotlining flag, which in turn enables the customer to make unrestricted calls.

In the fourth method step, the SC also communicates the secret key Ki_2 to the AC.

At this point, the card is released and provided with the final personalization.

5 The reuse of used cards is described in detail on page of the description. As seen from Fig. 3, the customer contacts with his card the VO which enters the card number ICCID into the order confirmation so that the IMSI is deleted both in the AC and in the HLR.

10 In this way, the key Ki_2 is deleted and the key Ki_1 is reactivated and stored in the card. Likewise, the PIN is set to the value 0000 and also the PUK.

The card, having been pre-personalized in this way, can now be sent to a card pool and reissued to new customers.

15

In other words, the final personalization is reversed so that the card is in the same state as when it was pre-personalized.

It should also be noted that the network operator where the order is placed, is also
20 referred to as Order Receiving Office and that this Order Receiving Office has knowledge of the association between ICCID and IMSI since the ICCID and IMSI have a 1:1 correspondence within the issued range of numbers.

Claims

1. Method for personalizing GSM chips having a memory range in which at least one subscriber identification number IMSI and a card number ICCID are stored, and
 5 wherein for personalizing the chip an additional secret key K_i and, optionally, additional data are stored, characterized in that the chip is personalized at the time when the subscriber logs on to the subscriber network.
- 10 2. The method according to claim 1, characterized in that the chip is personalized when the subscriber logs on to the subscriber network for the first time.
3. The method according to claim 1 or 2, characterized in that for pre-personalizing the chip at the manufacturer, at least initial, card-specific data, namely a first secret key
 15 K_{i_1} and, optionally, additional data, such as PIN and PUK are stored.
4. The method according to one of the claims 1-3, characterized by the following process steps:
 - in a first process step, the chip manufacturer obtains the ICCID and the IMSI
 20 from a number pool, the chip itself derives an initial key K_{i_1} from a key K_1 which is known to and entered into the chip by the chip manufacturer, while PIN and PUK are set to a default value,
 - in a second process step, an entry is made in the AC and HLR as soon as a subscriber has entered into a contract with the network operator,
 - 25 in a third process step, the AC also derives the initial first key K_{i_1} ,
 - in a fourth process step, the network sets the conditions so that during logon to the network, a connection is established from the chip to the component SC (security center of the network operator),
 - in a fifth process step, the connection is routed from the chip to the SC during
 30 the first logon,
 - in a sixth process step, a new, second secret key K_{i_2} and, optionally, a PUK is negotiated with the chip (for example using the Diffie-Hellman method) or generated in the SC and transmitted to the chip,

in a seventh process step, the conditions of the fourth process step are disabled again.

- 5 5. The method according to one of the claims 1-4, characterized in that the initial secret key Ki_1 which is first stored in the chip, is not transmitted to and stored in the authentication center (AC) before the contract is established.
- 10 6. Chip for carrying out the method according to one of the claims 1-5, characterized in that the chip in the terminal equipment is Toolkit-enabled and can communicate with the SC and negotiate a key.
- 15 7. The chip according to claim 6, characterized in that the chip can receive data from the SC and writes these data to its memory and, optionally, reads these data from the memory the and changes the data and/or transmits the data to the computer center (SC).
8. The chip according to one of the claims 6 or 7, characterized in that the micro-processor of the chip negotiates a secret key with the SC.
- 20 9. The chip according to claim 8, characterized in that the key of the method is negotiated using the Diffie-Hellman method.

10. The chip according to one of the claims 6-9, characterized in that the chip has a dialing number which is fixedly pre-programmed by the manufacturer (fixed dialing).

11. Computer center for carrying out the method according to one of the claims 1-5,
5 characterized in that the HLR is capable of setting and deleting a rerouting command (hotlining flag).

12. Computer center for carrying out the method according to one of the claims 1-5,
by using a chip according to one of the claims 6-10, characterized in that the network
10 sets conditions so that a connection is established from the chip to the component SC during logon to the network.

13. Computer center for carrying out the method according to one of the claims 1-5,
by using a chip according to one of the claims 6-10, characterized in that the hotlining
15 flag is set in the HLR when the initial key Ki_1 is a first entered in the AC.

SUMMARY

The invention relates to a method for personalization of GSM chips. At least one subscriber identification character (TMSI) and a card number (ICCID) are stored in the memory area of said chips in addition to a secret key (KI) and other optional data for personalization purposes. The invention aims to eliminate an unnecessarily high degree of complexity linked to management of all card data in an authentication centre (AC) and to preserve secret chip data in a more secure manner. According to the invention, final data is only written on the chip when the subscriber logs into a subscriber network. One advantage is that only initial data is written into the card enabling the customer to contact the computer centre of the information provider. During first contact the final data is traded between the card and the computer centre and written into the card. The computer centre is simply required to manage cards which have really been issued to customers.